Amendments to the Specification:

Please amend paragraph 4 on page 1 of the specification as follows:

Network browsers (browser applications), such as those commercially available from Netscape® ~~Navigator or~~and Microsoft® ~~Explorer~~, allow users of client machines to request and retrieve resources from remotely located server machines via the Internet. These network browsers can display or render HyperText Markup Language (HTML) documents provided by the remotely located server machines. Additionally, browsers are able to execute script programs embedded in the HTML documents to provide some local functionality.

Please amend paragraph 18 on page 6 of the specification as follows:

FIG. 1A is a block diagram of an information retrieval system 100 according to one embodiment of the invention. The information retrieval system 100 includes a network 102, client machines 104 and 106, an intermediary server 108, remote servers 110 and 112, a private network 114, and private servers 116 and 118. The network 102 serves as a communication medium through which the client machines 104 and 106, the intermediary server 108 and the remote servers 110 and 112 can communicate. The network 102 is, for example, a data network which can include the Internet, a wide area network, or a local area network. The Internet refers to a global network of interconnected computers. The private network 114 also serves as a communication medium through which the intermediary server 108 and the private servers 116 and 118 can communicate. The private network 114 is also a data network. Often the private network 114 is associated with an entity and thus employees operating computing devices on the private network 114 are able to communicate with the private servers 116 and 118, for example, the private network 114 can be referred to as a corporate network or an intranet. However, access to the private network 114 by an outside computing device is typically limited by a firewall (not

shown). The intermediary server 108 is permitted to communicate with the private network 114 through the firewall. Here, to the extent a client machine (requestor) is authorized and permitted, the intermediary server 108 communicates with the private network 114 on behalf of the client machine (requestor). The intermediary server 108, in effect, controls the extent to which it allows outside computing devices to access the private network 114.

Please amend paragraph 23 on page 8 of the specification as follows:

The information retrieval system 150 makes use of the Internet 152 and client machines 154 and 156 that couple to the Internet 152 through wired or wireless means. Typically, the client machines 154 and 156 operate client-side applications, such as a network browser or a mail application. When requestors (users) of the client machines 154 and 156 desire to access remote resources, resource requests are sent from the client machines 154 and 156 through the Internet 152 to an intermediary server 158. Typically, the communications between the client machines 154 and 156 and the intermediary server 158 are secured by an encryption technique (e.g., Secure Socket Layer (SSL)). The intermediary server 158 provides access to an intranet 160. The resources being requested by the client machines 154 and 156 reside within the intranet 160. Since a firewall typically limits or precludes external access to the intranet 160, the intermediary server 158 must be permitted to communicate with the intranet through the firewall 162. The intranet 160 typically includes various different types of resources that can be accessed electronically. Typically, these resources are stored on server machines that couple to, or form part of, the intranet 160. As shown in FIG. IB, the intranet 160 couples to, or includes, an authentication server 164, a web server 166, a mail server 168, a file server 170 and a log server 172. Hence, a given client machine can access any one of the servers 164-172 residing within or on the intranet 160 by way of the intermediary server 158. Consequently, a given client machine

can request and receive resources residing on the web server 166 using a network browser application. As another example, the given client machine can access the mail resources residing on the mail server 168 using a client-side mail application. As still another example, the given client machine can access the file server 170 residing within or on the intranet 160 to obtain, store or view electronic files thereon.

Please amend paragraph 26 on page 9 of the specification as follows:

The intermediary server 200 includes various processing modules typically implemented by computer program code executed by a processing device utilized by the intermediary server 200. More particularly, the processing modules of the intermediary server 200 include a web server 202 and a protocol handler 204. The web server 202 couples to client machines through a link 206 (via a network) and the protocol handler 204 couples to remote servers through a link 208 (via a network). The web server 202 and the protocol handler 204 also communicate with one another as well as with various supporting modules and a data storage device 210. The data storage device 210 provides persistent or non-volatile storage for various data items being maintained by the intermediary server 200. Typically, for each user or requestor associated with a client machine, the data storage device 210 provides separate storage.

Please amend paragraph 29 on page 10 of the specification as follows:

Another processing module that the intermediary server 200 might include is a cookie manager 218. The cookie manager 218 manages "cookies" such that those being received from a remote server are stored to the data storage device 210 and those "cookies" previously stored in the data storage device 210 are delivered to the remote server at appropriate times. More

generally, "cookies" refer to server stored information. Such server stored information is often set by a remote server and used for session, state or identification purposes.

Please amend paragraph 32 on page 11 of the specification as follows:

The intermediary server 252 also includes back-end protocol handlers 282. The back-end protocol handlers 282 provide the appropriate protocol for outgoing and incoming communications with respect to a particular server. The layer of back-end protocol handlers 282 shown in FIG. 2B includes protocol handlers for the protocols of: HTTP, IMAP, SMTP, POP, 5MB, NFS, NIS, RADIUS, LDAP, and NT. To the extent that an incoming protocol to the intermediary server 252 differs from an outgoing protocol from the intermediary server 252, the content transformer 278 can perform the protocol transformations (e.g., translations). Still further, the intermediary server 252 includes a data store 284, a log manager 286, and a data synchronization manager 288. The data store 284 can provide temporary or semipermanent data storage for the various components of the intermediary server 252. For example, a local record for authentication purposes can be stored for each of the clients or requestors in the data store 284. In addition, session identifiers, or cookies, for the clients or requestors can also be stored in a centralized fashion in the data store 284. The data synchronization manager 288 is a module that enables coupling of one intermediary server with another intermediary server to provide fault tolerance. Hence, if one intermediary server fails, then, through a link 290, the failing intermediary server can couple to an operating intermediary server to provide some or all of the operations typically associated with an intermediary server. The log manager 286 is provided to enable application level logging of various access requests that are made through the intermediary server 252. The log formed by the log manager 286 is stored in the log server 268.

Please amend paragraph 65 on page 22 of the specification as follows:

Initially, the host name for the appropriate remote server is obtained 902. In one embodiment, the host name can be obtained from storage. Here, the storage can, for example, be the data storage device [[214]] 210 illustrated in FIG. 2A. In another embodiment, the host name can be obtained from the URL associated with the web resource request. After the host name for the appropriate remote server is obtained 902, a host name lookup is performed 904 to obtain an IP address of the appropriate remote server. A connection is then opened 906 (or maintained if already opened) to the remote server. Next, a secure handshake is performed 908 between the intermediary server and the remote server as needed. Any "cookies" associated with the obtained host name are then obtained 910. Following the operation 910, the pre-processing of the web resource request at the intermediary server is complete and the request is now able to be forwarded to the remote server. At this point, the request for the web resource with associated "cookies" is sent 912 to the remote server.

Please amend paragraph 69 on page 24 of the specification as follows:

Next, certain URLs within an HTML portion of the response can be modified 936. In one embodiment, the modifications to the certain URLs can be achieved by modifying the host name portion of URLs within certain tags of the resulting HTML. In another embodiment, the modifications to the certain URLs can be achieved by adding suffixes to the certain URLs. The suffixes thus serve to allow the URLs to carry additional information. Further, certain URLs provided or produced by scripting language portions within the resulting HTML can be modified 938. Examples of scripting languages include JavaScript® and VBscript. In one embodiment, a host name portion of the certain URLs provided or produced by scripting language portions within the resulting HTML are modified 938. In another embodiment, the certain URLs

provided or produced by scripting language portions are modified 938 to include suffixes which carry supplemental information. Additional details on modifying scripting language portions is provided below with reference to FIGs, 13A and 13B. Thereafter, the modified response is sent 940 to the requestor.